

PATENT

MS146909.01/MSFTP118US



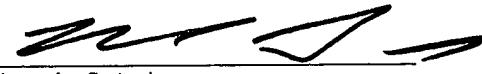
CERTIFICATE OF MAILING

I hereby certify that this correspondence (along with any paper referred to as being attached or enclosed) is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: **Mail Stop Appeal Brief – Patents**, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

EF
2131

4-25-05

Date


Himanshu S. Amin

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:

Applicants(s): Srivatsan Parthasarathy, *et al.*

Serial No: 09/605,602

Filing Date: June 28, 2000

Examiner: Michael R. Vaughan

Art Unit: 2131

Title: SHARED NAMES

**Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450**

APPEAL BRIEF

Dear Sir:

Applicant submits this brief in connection with an appeal of the above-identified patent application. A credit card payment form is filed concurrently herewith in connection with all fees due regarding this appeal brief. In the event any additional fees may be due and/or are not covered by the credit card, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1063 [MSFTP118US].

04/29/2005 EFLORES 00000080 09605602

01 FC:1402

500.00 OP

I. Real Party in Interest (37 C.F.R. §41.37(c)(1)(i))

The real party in interest in the present appeal is Microsoft Corporation, the assignee of the present application.

II. Related Appeals and Interferences (37 C.F.R. §41.37(c)(1)(ii))

Appellants, appellants' legal representative, and/or the assignee of the present application are not aware of any appeals or interferences which may be related to, will directly affect, or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims (37 C.F.R. §41.37(c)(1)(iii))

No claims have been withdrawn, canceled or allowed. Claims 1-24 stand rejected by the Examiner. The rejection of claims 1-24 is being appealed.

IV. Status of Amendments (37 C.F.R. §41.37(c)(1)(iv))

No claim amendments have been entered after the Final Office Action.

V. Summary of Claimed Subject Matter (37 C.F.R. §41.37(c)(1)(v))**A. Independent Claim 1**

Independent claim 1 recites a method for facilitating a secured name space for an assembly employable by application programs during runtime, comprising the steps of: providing a key pair having a public key and a private key; providing the assembly with a manifest that contains the public key; hashing the assembly; encrypting the hash of the assembly with the private key; and relating the encrypted hash to the assembly. (See, e.g. page 4, lines 14-19).

B. Independent Claim 9

Independent claim 9 recites a computer readable medium having at least one computer executable component employable by an application program at runtime comprising: an assembly including a manifest that contains a public key and a hash of the contents of the

assembly encrypted by a private key, the private key and the public key forming a key pair and the encrypted hash being referenced to the assembly. (*See, e.g.* page 4, lines 20-25).

C. Independent Claim 12

Independent claim 12 recites a system for facilitating secured name spaces of assemblies employable by application programs at runtime, the system comprising: a first component adapted to provide a manifest within an assembly with a public key; and a second component adapted to hash the contents of the assembly and encrypt the hash with a private key matching the public key. (*See, e.g.* page 4, line 26- page 5, line 1).

D. Independent Claim 19

Independent claim 19 recites a system for facilitating a secured name space of an assembly employable by application programs at runtime, the system comprising means for providing a key pair having a public key and a private key (*See, e.g.* Figure 5 and page 14, lines 5-6); means for inserting a public key in a manifest of an assembly (*See, e.g.* Figure 5 and page 14, lines 6-7); means for hashing the assembly (*See, e.g.* Figure 5 and page 14, lines 7-8); means for encrypting the hash of the assembly with the private key (*See, e.g.* Figure 5 and page 14, lines 8-9) and means for relating the encrypted hash to the assembly (*See, e.g.* Figure 5 and page 15, lines 10-14).

The aforementioned means for limitations are identified as claim elements subject to the provisions of 35 U.S.C. §112 ¶6. The corresponding structures are identified with reference to the specification and drawings in the parentheticals above corresponding to those claim limitations.

VI. Grounds of Rejection to be Reviewed (37 C.F.R. §41.37(c)(1)(vi))

A. Whether claims 1-24 stand rejected under 35 U.S.C. §102(e) as being anticipated by Renaud (US 6,021,491).

VII. Argument (37 C.F.R. §41.37(c)(1)(vii))

A. Rejection of Claims 1-24 Under 35 U.S.C. §102(e)

Claims 1-24 stand rejected under 35 U.S.C. §102(e) as being anticipated by Renaud (US 6,021,491). This rejection should be withdrawn for at least the following reasons. Renaud fails to disclose each and every limitation set forth in the subject claims.

A single prior art reference anticipates a patent claim only if it expressly or inherently describes *each and every limitation set forth in the patent claim*. *Trintec Industries, Inc. v. Top-U.S.A. Corp.*, 295 F.3d 1292, 63 USPQ2d 1597 (Fed. Cir. 2002); *See Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The *identical invention must be shown in as complete detail as is contained in the ... claim*. *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989) (emphasis added).

Independent claims 1, 9, 12 and 19 relate to providing security and facilitating integrity of components or assemblies employed during runtime by application programs. The subject independent claims recite similar limitations, namely: providing a key pair having a public key and a private key and *providing an assembly with a manifest that contains a public key*. In particular, for example, since the claimed invention provides the assembly with the public key-containing manifest, an unwanted user cannot access the assembly file, update it (e.g., possibly with a virus or any other sabotaging component), and publish the corrupted version of the assembly file, all the while impersonating the original publisher. Renaud does not allow for such enhanced transactional security as is provided for by the claimed invention.

Instead, Renaud teaches a digital signature verification system that employs a public/private key pair wherein a data file and signature file are provided to a user, and the user then verifies the digital signature in the signature file using a signature-verifying algorithm. However, instead of *storing a public key in a manifest of an assembly file* as in the claimed invention, the cited reference provides the public key to *all other users*. (See col. 1, lines 65-66). Therefore, the teachings of Renaud advance security defects that applicants' claimed invention in part strives to mitigate.

In the Final Office Action, the Examiner attempts to overcome the deficiencies of Renaud by incorrectly asserting that Schneier's *Applied Cryptography* combined with Renaud's teaching of "additional data" stored in the signature file (*i.e.* the name of the file, the file's author, the version of the file, a time-stamp, or a rating label. *See* col. 3, lines 39-42) suggests the claimed limitation of ***providing an assembly with a manifest that contains a public key***. However, the reference neither explicitly nor inherently discloses storing a public key in an assembly manifest. The additional data mentioned by Renaud simply relates to administrative information regarding contents of the file. There is no suggestion that the additional data can be a public key. Consequently, the cited reference does not ***provide an assembly with a manifest that contains a public key***, as is afforded by the claimed invention. The Examiner is reminded that the standard by which anticipation is to be measured is ***strict identity*** between the cited document and the invention as claimed, not mere equivalence or similarity. *See, Richardson* at 9 USPQ2d 1913, 1920.

In view of at least the foregoing, it is readily apparent that Renaud does not anticipate or suggest applicants' invention as recited in the subject claims. Accordingly, this rejection with respect to independent claims 1, 9, 12 and 19 (and the claims that depend there from) should be withdrawn.

B. Conclusion

For at least the above reasons, the claims currently under consideration are believed to be patentable over the cited reference. Accordingly, it is respectfully requested that the rejections of claims 1-24 be reversed.

If any additional fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP118US].

Respectfully submitted,
AMIN & TUROCY, LLP



Himanshu S. Amin
Reg. No. 40,894

AMIN & TUROCY, LLP
24th Floor, National City Center
1900 East 9th Street
Telephone: (216) 696-8730
Facsimile: (216) 696-8731

VIII. Claims Appendix (37 C.F.R. §41.37(c)(1)(viii))

1. A method for facilitating a secured name space for an assembly employable by application programs during runtime, comprising the steps of:
 - providing a key pair having a public key and a private key;
 - providing the assembly with a manifest that contains the public key;
 - hashing the assembly;
 - encrypting the hash of the assembly with the private key; and
 - relating the encrypted hash to the assembly.
2. The method of claim 1, further comprising the step of providing a referencing assembly that references the assembly with a manifest that contains a token of the public key.
3. The method of claim 2, further comprising the step of determining if the contents of the assembly has been modified by decoding the encrypted hash value with the public key, determining an actual hash of the contents of the assembly and comparing the decoded encrypted hash with the actual hash.
4. The method of claim 3, further comprising the step of determining if the publisher of the assembly is the owner of the private key.
5. The method of claim 4, the step of determining if the publisher of the assembly is the original owner of the key pair comprising the step of comparing the token of the public key in the referencing assembly with the public key stored in the manifest of the assembly.
6. The method of claim 1, further comprising the step of determining if the contents of the assembly has been modified by decoding the encrypted hash value with the public key, determining an actual hash of the contents of the assembly and comparing the decoded encrypted hash with the actual hash.

7. The method of claim 6, further comprising the step of determining if the publisher of the assembly is the original owner of the key pair.

8. The method of claim 7, the step of determining if the publisher of the assembly is the original owner of the key pair comprising the step of storing the public key in a storage medium and comparing the public key in the storage medium with the public key in the manifest.

9. A computer readable medium having at least one computer executable component employable by an application program at runtime comprising:

an assembly including a manifest that contains a public key and a hash of the contents of the assembly encrypted by a private key, the private key and the public key forming a key pair, the encrypted hash being referenced to the assembly.

10. The computer readable medium of claim 9, further including a referencing assembly that references the assembly, the referencing assembly including a manifest that contains a token of the public key of the assembly.

11. The computer readable medium of claim 9, the assembly being a dynamically linked library.

12. A system for facilitating secured name spaces of assemblies employable by application programs at runtime, the system comprising:

a first component adapted to provide a manifest within an assembly with a public key; and

a second component adapted to hash the contents of the assembly and encrypt the hash with a private key matching the public key.

13. The system of claim 12, further comprising a third component adapted to provide a token of the public key to a manifest of a referencing assembly that references the assembly.

14. The system of claim 13, further comprising a verification component adapted to decode the encrypted hash with the public key and compare the decoded encrypted hash with an actual hash run on the assembly.
15. The system of claim 14, the verification component being further adapted to compare the public key in the manifest of the assembly with the token of the public key in the manifest of the referencing assembly.
16. The system of claim 12, further comprising a key pair generating component adapted to generate a key pair.
17. The system of claim 12, further comprising a binding component adapted to provide binding policy information for determining a version of an assembly that an application program will run if another assembly having the same name resides on the system.
18. The system of claim 12, further comprising a verification component adapted to decode the encrypted hash with the public key and compare the decoded encrypted hash with an actual hash run on the assembly.
19. A system for facilitating a secured name space of an assembly employable by application programs at runtime, the system comprising:
 - means for providing a key pair having a public key and a private key;
 - means for inserting a public key in a manifest of an assembly;
 - means for hashing the assembly;
 - means for encrypting the hash of the assembly with the private key; and
 - means for relating the encrypted hash to the assembly.
20. The system of claim 19, further comprising means for providing a token relating to the public key and means for inserting the token into a manifest of a referencing assembly that references the assembly

21. The system of claim 20, further comprising means for determining if the assembly has been modified.
22. The system of claim 21, the means for determining if the assembly has been modified including means for decoding the encrypted hash with the public key, means for generating an actual hash value and means for comparing the generated hash value with the decoded encrypted hash value.
23. The system of claim 22, further comprising means for comparing the token in the referencing assembly with the public key in the assembly.
24. The system of claim 19, at least one of the assembly and referencing assembly being a dynamically linked library.

IX. Evidence Appendix (37 C.F.R. §41.37(c)(1)(ix))

None.

X. Related Proceedings Appendix (37 C.F.R. §41.37(c)(1)(x))

None.